Ministerie van Justitie en Veiligheid

Jaarrapportage Functionaris Gegevensbescherming Passagiersinformatie-eenheid Nederland

2022

Datum *24 mei 2023*
Status *definitief*

Colofon

Afzendgegevens	**Minister van Justitie en Veiligheid** Turfmarkt 147 2511 DP Den Haag Postbus 20301 2500 EH Den Haag www.rijksoverheid.nl/jenv
Contact	T 070 370 68 89
Bijlage(n)	-
Auteurs	Functionaris voor gegevensbescherming Pi-NL FG-Pi-NL@minjenv.nl

Inhoud

1 Inleiding

Voor u ligt de jaarrapportage over het jaar 2022 van de functionaris voor gegevensbescherming van de Passagiersinformatie-eenheid Nederland (hierna: FG). Deze rapportage vindt zijn grondslag in artikel 18, lid 2 van de Wet gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven (hierna: PNR-wet). Hierin is bepaald dat de FG jaarlijks voor 1 juli een rapportage zendt aan de minister van Justitie en Veiligheid, de beide Kamers der Staten-Generaal en de Autoriteit Persoonsgegevens over het voorgaande kalenderjaar. In deze rapportage gaat de FG in op de wijze waarop controle is uitgeoefend op de verwerking van de persoonsgegevens door de Passagiersinformatie-eenheid Nederland (hierna: Pi-NL) en de wijze waarop de waarborgen voor de gegevensbescherming zijn uitgevoerd. De rapportage bevat tevens statistieken over de mate waarin passagiersgegevens op grond van de artikelen 9a tot en met 16 van de PNR-wet zijn verstrekt, doorgegeven of verzocht.

Over de passagiersinformatie-eenheid Nederland

Op 18 juni 2019 is de PNR-wet in werking getreden. De wet implementeert de Richtlijn 2016/681/EU van het Europees Parlement en de Raad van 27 april 2016 over het gebruik van persoonsgegevens van passagiers voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit. Deze PNR-richtlijn voorziet in een verplichting voor de lidstaten om een passagiersinformatie-eenheid in te richten en luchtvaartmaatschappijen voor te schrijven dat zij passagiersgegevens van vluchten waarover zij voor hun normale bedrijfsvoering beschikken, te versturen naar de passagiersinformatie-eenheid van de lidstaat waarvan of waarnaar een vlucht plaatsvindt.

Onder de verantwoordelijkheid van de minister van Justitie en Veiligheid heeft de Pi-NL de volgende taken:

- Het beoordelen van de passagiers voorafgaand aan hun geplande aankomst in of geplande vertrek uit Nederland, om te bepalen welke personen vanwege mogelijke betrokkenheid bij een terroristisch of ernstig misdrijf moeten worden onderworpen aan een nader onderzoek door een bevoegde instantie of Europol;
- Het voldoen aan een vordering van gegevens van een bevoegde instantie of aan een verzoek van Europol;
- Het analyseren van passagiersgegevens voor het opstellen van nieuwe of het bijstellen van bestaande criteria die worden gebruikt bij de beoordelingen om te bepalen welke personen betrokken zouden kunnen zijn bij een terroristisch of ernstig misdrijf.

De FG is belast met de controle op deze verwerkingen van persoonsgegevens door de Passagiersinformatie-eenheid en met de controle op de uitvoering van de desbetreffende waarborgen voor de gegevensbescherming.

2 Samenvatting

Vooraf: de huidige functionaris gegevensbescherming van de Pi-NL is gestart in februari 2023. Derhalve is voorliggende rapportage goeddeels gebaseerd op de bevindingen van zijn voorganger die tot en met oktober 2022 werkzaam was als FG Pi-NL, aangevuld met observaties van en navraag door de huidige FG. De rapportage is vooraf doorgesproken met de Pi-NL, de Koninklijke Marechaussee (waar de Pi-NL fysiek en beheersmatig is ondergebracht) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (die beleidsmatig en financieel verantwoordelijk is voor de Pi-NL).

Samenvattend kan worden gesteld dat het management en de medewerkers van de Pi-NL zich bewust zijn van het belang van gegevensbescherming en zorgvuldig omgaan met de persoonsgegevens die zij verwerken. De wettelijke waarborgen voor het beschermen van persoonsgegevens die zijn gecontroleerd, zijn aanwezig en functioneren voldoende. 'Voldoende' impliceert echter ook dat er nog verschillende verbeterpunten zijn. De belangrijkste hiervan zijn:

- De Pi-NL zou baat hebben bij een meer geïntegreerde en gedocumenteerde privacy-aanpak. De basis is op orde maar voor verdere continue verbetering van de privacy-waarborgen ontbreken nog een helder privacy-raamwerk, vastgelegde werkwijzen en continue monitoring en verbetering hiervan.
- De Pi-NL dient uitvoering te geven aan de uitspraak van het Hof van Justitie van de Europese Unie van 21 juni 2022[1], specifiek ten aanzien van de bewaartermijn van passagiersgegevens en de selectie van intra-Europese vluchten waarvan de gegevens worden verwerkt.

[1] Prejudiciële beslissing van het Hof in het kader van een geding tussen de Ligue des droits humains en de Ministerraad (België) over de rechtmatigheid van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens. HvJ EU 21 juni 2022, C-817/19, ECLI:EU:C:2022:491

3 Waarborgen en bevindingen

De PNR-wet bevat verschillende waarborgen voor het beschermen van passagiersgegevens. In deze wet is tevens een aantal waarborgen uit de Wet politiegegevens (hierna: Wpg) van overeenkomstige toepassing verklaard. Hieronder volgt een beknopte weergave van deze waarborgen (in verband met de leesbaarheid wordt steeds een samenvatting van de wettelijke vereisten gegeven) en de bevindingen van de FG ten aanzien van aanwezigheid en werking van deze waarborgen. De wijze waarop de controle is uitgeoefend bestond uit het inspecteren van beleidsdocumenten, procedures en werkinstructies, het vaststellen of conform deze opzet wordt gewerkt, het inspecteren van procedures en instellingen in gebruikte systemen, het inspecteren van 'logbestanden' (overzichten van gedane verwerkingen), het inspecteren van diverse registratiesystemen (zoals melding van datalekken) en auditrapporten, het doen van steekproeven (bijvoorbeeld ten aanzien van afscherming van persoonsgegevens na zes maanden), interviews en observaties op de werkvloer.

Functionaris voor gegevensbescherming (art 18 PNR-wet en art 36 Wpg)
De PNR-wet vereist de benoeming van een FG voor de Pi-NL door de verwerkingsverantwoordelijke (de minister van Justitie en Veiligheid). De FG ziet toe op de naleving van de relevante bepalingen uit de PNR-wet en de Wpg, op de toewijzing van autorisaties, op de bewustmaking en opleiding van de medewerkers van de Pi-NL die zijn betrokken bij de verwerking van passagiersgegevens en op de audits. De FG informeert en adviseert daarnaast de verwerkingsverantwoordelijke en de medewerkers van de Pi-NL over wettelijke gegevensbeschermingsbepalingen en over de gegevensbeschermingseffectbeoordeling. Ook werkt de FG samen met de Autoriteit Persoonsgegevens. Verder is de FG voor een betrokkene het contactpunt voor alle aangelegenheden in verband met de verwerking van de persoonsgegevens van die betrokkene door de verwerkingsverantwoordelijke. De FG dient voor de uitvoering van diens taken toegang te hebben tot alle gegevens die door de Pi-NL worden verwerkt. De FG kan de Autoriteit Persoonsgegevens informeren indien hij vaststelt dat een verwerking van persoonsgegevens door de Pi-NL niet rechtmatig is. De FG wordt door de verwerkingsverantwoordelijke tijdig en naar behoren betrokken bij alle aangelegenheden die verband houden met de bescherming van passagiersgegevens.

Bevindingen 2022: Er was een FG voor de Pi-NL benoemd en ook aangemeld bij de Autoriteit Persoonsgegevens. De FG heeft voor betrokkenen als contactpunt gefungeerd en had toegang tot alle noodzakelijke gegevens. Er heeft regelmatig contact plaatsgevonden tussen de FG, management en medewerkers Pi-NL en de NCTV. Ook heeft de FG een actieve rol gehad in de bewustmaking en advisering van medewerkers en management van de Pi-NL ten aanzien van interpretatie en toepassing van wettelijke gegevensbeschermingsbepalingen. De FG heeft verder een actieve rol gehad in het oprichten van en participeren in een Europees kennisuitwisselingsplatform van en voor FG's van de verschillende passagiersinformatie-eenheden. Er is geen contact geweest met de Autoriteit Persoonsgegevens.

Verbod op verwerken van bijzondere gegevens (art 19 PNR-wet)
De PNR-wet verbiedt het maken van onderscheid op grond van bijzondere persoonsgegevens, zoals ras, etnische afkomst, godsdienst of gezondheid.

Bevindingen 2022: Wanneer een luchtvaartmaatschappij bijzondere gegevens aanlevert, verwijdert het geautomatiseerde filtersysteem van TRIP de als zodanig aangemerkte gegevens; deze worden daarmee niet verder verwerkt door de Pi-NL. Aandacht van de Pi-NL blijft benodigd voor het steekproefsgewijs controleren van de dataset op bijzondere gegevens en het actualiseren van de lijst met woorden en kenmerken die vallen onder bijzondere gegevens.

Bewaartermijn en afscherming (art 20 PNR-wet)
De PNR-wet stelt dat de passagiersgegevens gedurende een termijn van vijf jaar na ontvangst van deze gegevens worden bewaard en dat de passagiersgegevens na deze termijn worden gewist. De ontvangen passagiersgegevens dienen te worden opgeslagen en verwerkt in Nederland of in een andere lidstaat van de Europese Unie. De passagiersgegevens waaruit rechtstreeks de identiteit van een persoon kan worden afgeleid, dienen zes maanden na ontvangst ervan te worden gedepersonaliseerd door afscherming van die gegevens. Daarna kunnen deze gegevens uitsluitend worden doorgegeven met toestemming van de officier van justitie en na kennisgeving aan de functionaris gegevensbescherming, die deze verwerking achteraf controleert.

Bevindingen 2022: Het automatisch depersonaliseren van passagiersgegevens in TRIP functioneert en de FG controleert dit periodiek. De FG ontvangt een notificatie bij doorgifte van persoonsgegevens ouder dan zes maanden. In 2022 is in een aantal gevallen geen notificatie verzonden. Oorzaken waren het verkeerd administreren van de vordering of het verzoek door de bevoegde instantie waardoor de notificatie uitbleef en aanpassing van de software waardoor notificatie (tijdelijk) uitbleef. De FG heeft de verstrekkingen op basis van de notificaties gecontroleerd en geconstateerd dat in alle gevallen toestemming van de officier van justitie voor depersonalisatie aanwezig was. De FG kan het functioneren van de bewaartermijn van vijf jaar (en het daarna wissen van deze gegevens) in de praktijk nog niet controleren aangezien er pas sinds juni 2019 passagiersgegevens worden opgeslagen.

Een aandachtspunt met betrekking tot de bewaartermijn betreft de uitspraak van het Hof van Justitie van de Europese Unie van 21 juni 2022. Hierin stelt het Hof in punt 262:

"[…] *dat artikel 12, lid 1, van de PNR-richtlijn, gelezen in samenhang met de artikelen 7 en 8 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen nationale wetgeving die voor PNR-gegevens een algemene bewaartermijn van vijf jaar voorschrijft die zonder onderscheid geldt voor alle luchtreizigers, ook luchtreizigers van wie noch uit de voorafgaande beoordeling [artikel 6, lid 2, onder a), van deze richtlijn], noch uit eventuele controles tijdens de periode van zes maanden (artikel 12, lid 2, van deze richtlijn), noch uit andere omstandigheden is gebleken dat er objectieve aanwijzingen bestaan dat zij een gevaar vormen op het gebied van terroristische misdrijven of ernstige criminaliteit met een minstens indirect objectief verband met het luchtvervoer van passagiers*"

Het Hof geeft daarbij in punt 259 aan:

"*Wanneer in specifieke gevallen op basis van objectieve elementen, zoals PNR-gegevens die een geverifieerde positieve overeenkomst opleveren, kan worden aangenomen dat bepaalde reizigers een risico kunnen vormen op het gebied van terrorisme of ernstige criminaliteit, lijkt het echter wel toelaatbaar hun PNR-gegevens langer dan die initiële periode op te slaan*" (waarbij de 'initiële periode' doelt op de bewaartermijn van zes maanden)

De verwerkingsverantwoordelijke en de Pi-NL hebben in 2022 in overleg met de bevoegde instanties deze uitspraak nader geanalyseerd en oplossingsrichtingen geformuleerd. De vraag en oproep aan de verwerkingsverantwoordelijke (minister JenV) en de Pi-NL is nu hoe zij concrete invulling gaan geven aan deze uitspraak van het Hof, aangezien de bestaande nationale wet, conform de richtlijn, een algemene bewaartermijn van vijf jaar voorschrijft.

Register (art 22 PNR-wet)
De verwerkingsverantwoordelijke dient een register bij te houden dat gegevens bevat met betrekking tot de Pi-NL en andere passagiersinformatie-eenheden in de EU, bevoegde instanties en toegekende autorisaties. Verder draagt de verwerkingsverantwoordelijke zorg voor de vastlegging van verzoeken om passagiersgegevens van bevoegde instanties, Europol en andere passagiersinformatie-eenheden.

Bevindingen 2022: de betreffende informatie is aanwezig en opvraagbaar bij de Pi-NL.

Vastleggen verwerkingen (art 23 PNR-wet)
De verwerkingsverantwoordelijke dient zorg te dragen voor de vastlegging langs elektronische weg van ten minste de volgende verwerkingen: het verzamelen, raadplegen, verstrekking onder meer in de vorm van doorgiften en wissen van de passagiersgegevens en de resultaten van de verwerking van die gegevens.

Bevindingen 2022: Genoemde verwerkingen worden elektronisch vastgelegd in het TRavel Information Portal (TRIP) systeem van Pi-NL.

Menselijke toets (art 8 PNR-wet)
Indien een geautomatiseerde vergelijking van passagiersgegevens met een vordering, databank of criteria een positieve overeenkomst oplevert, moet deze door menselijke tussenkomst worden gecontroleerd om te bepalen of een bevoegde instantie maatregelen moet treffen of nader onderzoek moet doen.

Bevindingen 2022: de menselijke toets na positieve overeenkomst op grond van een geautomatiseerde vergelijking wordt door het systeem geautomatiseerd afgedwongen.

Juistheid en volledigheid gegevens (art 4 Wpg)
De verwerkingsverantwoordelijke treft de nodige maatregelen opdat de passagiersgegevens juist en nauwkeurig zijn.

Bevindingen 2022: Naast de Passenger Name Records (PNR) die luchtvaartmaatschappijen verzamelen en aan de Pi-NL doorgeven, kunnen zij in een aantal gevallen ook beschikken over Advance Passenger Information (API-gegevens). Vaak bevatten deze laatste gegevens geautomatiseerd ingelezen paspoortinformatie. In vergelijking met PNR (die deels door de passagier bij boeking zelf wordt ingevuld) betreft het dan *extra* en in veel gevallen ook *geverifieerde* informatie. De API-gegevens kunnen daarmee positief bijdragen aan het identificeren van passagiers en aan het voorkomen van het onnodig verstrekken van passagiersgegevens. Maar de API-gegevens worden nog niet van alle luchtvaartmaatschappijen ontvangen.

Ander aandachtspunt is de formalisatie door het Openbaar Ministerie van zogenaamde ‘spoedvorderingen’ die bij de Pi-NL zijn ingediend. Deze formalisatie

dient volledieger en tijdiger door de betreffende officieren van justitie plaats te vinden. Ondanks de herinneringen die Pi-NL hiertoe uitstuurt en het overleg dat hierover heeft plaatsgevonden tussen Pi-NL en het Openbaar Ministerie, vond deze formalisatie in 2022 nog te vaak niet of buiten de gestelde termijn van 72 uur plaats.

Gegevensbescherming door beveiliging en ontwerp (art 4a Wpg)
De bescherming van de passagiersgegevens dient door technische en organisatorische maatregelen te zijn gewaarborgd.

Bevindingen 2022: Het kernsysteem van de Pi-NL, het TRavel Information Portal (TRIP), is volgens de principes van 'gegevensbescherming door beveiliging en ontwerp' gebouwd en ingericht. De Commandant van de Koninklijke Marechaussee, de beheersmatig verantwoordelijke voor de Pi-NL, heeft verder een 'Statement of Compliance' afgegeven voor de genomen technische en organisatorische maatregelen ter bescherming van passagiersgegevens. Aandachtspunten hierbij zijn wel de verwerking van passagiersgegevens buiten het TRIP-systeem om (zie ook kopje 'Audit'), de noodzaak om ook van de andere verwerkende partijen de bevestiging te ontvangen dat zij aan de gestelde beveiligingseisen voldoen (zie ook kopje 'Verwerkers') en het nog niet aanwezig zijn van controles op het verwerken van passagiersgegevens alleen op de daarvoor aangewezen locaties.

Verder beschikt Pi-NL nog niet over een overkoepelend privacyraamwerk en -beleid en formele, vastgelegde processen daarin. Geadviseerd wordt toe te werken naar een dergelijk raamwerk, met bijbehorende beheerprocessen (structurele monitoring, evaluatie en rapportage). Onderdeel van dit raamwerk zou een *toetsbaar normenkader* moeten zijn. In een dergelijk kader worden voor alle relevante wettelijke bepalingen in de PNR-wet en Wpg de interne beheersingsmaatregelen benoemd, inclusief de wijze waarop deze maatregelen worden getoetst[2]. Op deze wijze kan meer gedocumenteerd en planmatig invulling worden gegeven aan de bescherming van passagiersgegevens.

Gegevensbescherming door standaardinstellingen (art 4b Wpg)
Passagiersgegevens mogen alleen worden verwerkt voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische en ernstige misdrijven en deze gegevens mogen niet zonder tussenkomst van een natuurlijke persoon voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.

Bevindingen 2022: Aan deze waarborg wordt voldaan; een aandachtspunt hierbij is wel de uitspraak van het Hof van Justitie van de Europese Unie van 21 juni 2022 ten aanzien van intra-Europese vluchten. Het Hof geeft in punt 173 van zijn arrest aan:

"*Wordt de betrokken lidstaat niet met een werkelijke en actuele of voorzienbare terroristische dreiging geconfronteerd, dan kan daarentegen niet worden geoordeeld dat het ongedifferentieerd toepassen van het systeem van de PNR-richtlijn – én op vluchten naar of vanuit derde landen én op vluchten binnen de EU – beperkt is tot het strikt noodzakelijke*."

De verwerkingsverantwoordelijke en de Pi-NL hebben zoals eerder aangegeven in 2022 in overleg met de bevoegde instanties de uitspraak van het Hof nader geanalyseerd en oplossingsrichtingen geformuleerd. De verwerkingsverantwoordelijke en Pi-NL zullen nu een systeem moeten

[2] Een nuttig aanknopingspunt hiervoor kan worden gevonden in de Handreiking Privacy audit Wet politiegegevens voor Boa's van de Nederlandse Orde van Register EDP-Auditors (NOREA)

implementeren waarbij het verwerken van passagiersgegevens van intra-EU vluchten tot het strikt noodzakelijke is beperkt. Dit systeem was in 2022 nog niet ingevoerd.

Gegevensbeschermingseffectbeoordeling (art 4c Wpg)
Voorafgaande aan de verwerking van de passagiersgegevens moet een beoordeling zijn uitgevoerd van het effect van de voorgenomen verwerkingsactiviteiten op de bescherming van persoonsgegevens.

Bevindingen 2022: Deze beoordeling is uitgevoerd; aandachtspunt hierbij is dat deze gegevensbeschermingseffectbeoordeling voor het laatst is geactualiseerd in mei 2020; de verwerkingsverantwoordelijke wordt geadviseerd om dit op korte termijn opnieuw te doen.

Autorisaties en toegang (art 6 en 6a Wpg)
De verwerkingsverantwoordelijke dient een systeem van autorisaties te onderhouden dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid.

Bevindingen 2022: in 2022 werkte de Pi-NL met een systeem van 'rolgebaseerde autorisaties'. Mede op advies van de FG is in dat jaar gestart met het opzetten van een functiegericht autorisatiesysteem. Hiermee kunnen autorisaties transparanter, zorgvuldiger en meer gericht ('need-to-know' basis) worden toegekend. Het systeem was in 2022 nog niet geïmplementeerd; er zijn derhalve nog geen bevindingen over de werking ervan. Geadviseerd wordt het nieuwe autorisatiesysteem zo snel mogelijk in te richten.

Verwerkers (art 6c Wpg)
Ook de partijen die passagiersgegevens verwerken ten behoeve van de Pi-NL dienen passende technische en organisatorische maatregelen en procedures te hebben geïmplementeerd zodat bij de verwerking wordt voldaan aan de PNR-wet en de van overeenkomstige verklaarde artikelen uit de Wpg. De uitvoering van verwerkingen door een verwerker dient te zijn geregeld in een schriftelijke overeenkomst.

Bevindingen 2022: er zijn in 2019 verwerkersafspraken ("Verwerkersafspraak PNR-gegevens, 17 juni 2019") gemaakt tussen Pi-NL, de Justitiële Informatiedienst van het ministerie van Justitie en Veiligheid en het Joint IV Commando van het ministerie van Defensie. Aandachtspunt hierbij is dat ook deze verwerkers (die niet onder het toezicht van de FG Pi-NL vallen) moeten blijven aantonen dat wordt voldaan aan alle gestelde waarborgen voor het beschermen van persoonsgegevens. Advies aan de verwerkingsverantwoordelijke en de Pi-NL is deze waarborgen en bijbehorende technische en organisatorische maatregelen met betreffende verwerkers verder uit te werken en de bevestiging van de werking hiervan periodiek op te vragen en te (laten) controleren bij de verwerkers.

Rechten van betrokkene (art 24a t/m 31c Wpg)
Een betrokkene (een luchtvaartpassagier) dient duidelijke informatie over de verwerking van passagiersgegevens te ontvangen en, op diens schriftelijke verzoek, binnen zes weken uitsluitsel over de verwerking van hem betreffende persoonsgegevens. Betrokkene kan deze gegevens laten rectificeren of vernietigen indien deze niet juist zijn (verwerkt).

Bevindingen 2022: De bedoelde informatie is beschikbaar op de website rijksoverheid.nl/onderwerpen/luchtvaart/reisgegevens-luchtvaart. In 2022 zijn 43 inzageverzoeken van betrokkenen afgehandeld. De FG heeft opgetreden als contactpunt voor alle betrokkenen.

Het advies is om op de website nog duidelijker te maken dat de Pi-NL een *vergelijkende* functie heeft (vergelijken van passagiersgegevens met databanken, vorderingen etc.) en niet zelf *signaleert.* Berichten uit de media en vragen van betrokkenen maken duidelijk dat het vaak voor mensen niet duidelijk is wat precies de rol van de Pi-NL is en die van de bevoegde instanties, zoals politie en Koninklijke Marechaussee.
Verder wordt geadviseerd om ná het eerste contact dat betrokkenen met de FG leggen, in de vervolgcommunicatie (besluiten, vragen) het contact direct tussen de Pi-NL en de betrokkenen te laten plaatsvinden. Dit voorkomt nodeloze handelingen, draagt bij aan dataminimalisatie en versnelt en verduidelijkt het proces voor betrokkenen. De FG, Pi-NL en verwerkingsverantwoordelijke zullen hier nadere afspraken over moeten maken.

Audits (art 33 Wpg)
Vierjaarlijks dient een *privacy audit* plaats te vinden bij de Pi-NL en jaarlijks een *interne audit* ter voorbereiding op de privacy audit. De privacy audit heeft betrekking op de wijze waarop het verwerken van passagiersgegevens is georganiseerd, de maatregelen en procedures die daarop van toepassing zijn en de werking van deze maatregelen en procedures.

Bevindingen 2022: In 2022 heeft een interne audit plaatsgevonden. De conclusie van de auditor hierbij was dat: "Door het ontbreken van (actuele) documentatie waarin proces en/of beleid omschreven wordt dat invulling geeft aan de opzet van de diverse beheersmaatregelen gerelateerd aan de normen waarop de audit heeft plaatsgevonden, de toets op de opzet van deze beheersmaatregelen gerelateerd niet is geslaagd. Als gevolg van het niet slagen van de toets op de opzet, heeft er geen toetsing plaats kunnen vinden op bestaan en werking van beheersmaatregelen. Zonder de juiste opzet zal het bestaan en de werking van beheersmaatregelen immers op toeval berusten, in plaats van op een gestandaardiseerd, herhaalbaar, gecontroleerd proces." De auditor heeft in een aanvullend rapport enkele extra observaties gedeeld, met hieraan gekoppeld ook enkele adviezen.

De FG adviseert de benodigde documentatie op korte termijn aan te vullen, de aanbevelingen uit de interne audit uit te voeren en alsnog een controle uit te voeren. Hierbij ook het advies om op systematische wijze dergelijke bevindingen intern te agenderen, een verantwoordelijk medewerker en MT-lid aan te koppelen en de voortgang op (het invulling geven aan) de aanbevelingen te monitoren. Zie ook het advies onder het kopje 'Gegevensbescherming door beveiliging en ontwerp'.

Melding datalekken (art 33a Wpg)
De verwerkingsverantwoordelijke meldt een inbreuk op de beveiliging direct en uiterlijk binnen 72 uur nadat hij ervan heeft kennisgenomen aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden van personen met zich meebrengt.

Bevindingen 2022: Door de Pi-NL zijn in 2022 vier inbreuken op de beveiliging gemeld aan de privacy coördinator van de NCTV. De privacy coördinator heeft drie van deze vier meldingen beoordeeld als datalek. Naar oordeel van de privacy coördinator was hiervan geen melding bij de Autoriteit Persoonsgegevens benodigd. Eén datalek betrof verkeerde informatie die was doorgegeven aan een andere passagiersinformatie-eenheid. De data is daar niet gebruikt en direct verwijderd. Twee gevallen betroffen te veel PNR-gegevens die waren verstrekt aan een Nederlandse bevoegde instantie ten opzichte van de selectie die de instantie bevoegd was te ontvangen. Betreffende instanties hebben bevestigd dat de te veel

verstrekte informatie niet is gebruikt en is verwijderd. Naar aanleiding van deze gevallen zijn bestaande processen en werkinstructies bij de Pi-NL gecontroleerd en waar nodig aangevuld en intern gecommuniceerd.

CONCLUSIE

De wettelijke waarborgen voor het beschermen van persoonsgegevens zijn aanwezig in het primaire proces. Ook de interne cultuur en actiebereidheid om passagiersgegevens te beschermen zijn aanwezig bij de Pi-NL. Er zijn nog wel verschillende aandachtspunten onderkend, waaronder de tijdige formalisatie van spoedvorderingen, het volledig verzamelen van API-gegevens, implementatie van een gerichter autorisatiesysteem, opvolging geven aan de interne audit 2022 en het actualiseren van de gegevensbeschermingseffectbeoordeling uit 2020. De belangrijkste aandachtspunten en adviezen betreffen het toewerken naar een meer geïntegreerde en gedocumenteerde privacy-aanpak en het uitvoering geven aan de uitspraak van het Hof van Justitie van de Europese Unie over de PNR-richtlijn.

4 Statistieken

Hieronder volgen de statistieken over de mate waarin passagiersgegevens op grond van de artikelen 9a tot en met 16 van de PNR-wet zijn verstrekt, doorgegeven of verzocht in 2022.

Toelichting:
In onderstaande tabel worden de volgende afkortingen gebruikt:

- BINL: Nederlandse bevoegde instantie, zoals vermeld in de PNR-wet (het Openbaar Ministerie, de politie, de bijzondere opsporingsdiensten, de Koninklijke Marechaussee en de Rijksrecherche).
- OvJ: officier van justitie
- PIU: Passenger Information Unit, te weten een passagiersinformatie-eenheid uit een andere lidstaat
- BIEU: Bevoegde instantie uit een Europese lidstaat.

Nota bene 1: Op dit moment verstrekt de Pi-NL niet rechtstreeks aan derde landen. Indien een derde land om passagiersgegevens verzoekt, verloopt dit via een internationaal rechtshulpverzoek aan het (Landelijk) Internationaal Rechtshulp Centrum.
Nota bene 2: één vordering kan in de praktijk tot nul, een of meerdere verstrekkingen leiden (bijvoorbeeld omdat een passagier meerdere vluchten heeft gemaakt).

1	**Vorderingen**	
1.1	Totalen algemeen	
1.1.1	Totaal aantal vorderingen	**3.856**
1.1.2	Totaal aantal vorderingen met toestemming OvJ demaskeren	**893**
	BINL – PINL (art 9 PNR)	
1.2	Aantal vorderingen van BINL aan PINL	
1.2.1	Aantal ontvangen vorderingen van BINL	**2.928**
1.2.2	Aantal vorderingen met toestemming OvJ demaskeren	**733**
	BINL - PINL - PIU - PINL – BINL (art 14 PNR lid 2 en 3)	
1.3	Aantal verzoeken door PINL bij PIU t.b.v. BINL	
1.3.1	Aantal ontvangen vorderingen van BINL met verzoek aan PIU	**339**
1.3.2	Aantal vorderingen met toestemming OvJ demaskeren	**103**
1.3.3	Aantal door Pi-NL verstuurde verzoeken aan PIU t.b.v. BINL	**294**

	BINL - PIU – BINL (art 16 PNR lid 1 en 2)	
1.4	Aantal door BINL rechtstreeks verstuurde verzoeken aan PIU in het kader van dringende noodzaak	
1.4.1	Aantal ontvangen afschriften van verzoek BINL verzonden door PIU	**0**
	PIU- PIU (art 10 PNR lid 2)	
1.5	PIU - PIU	
1.5.1	Ontvangen verzoeken van PIU	**805**
1.5.2	Aantal verzoeken PIU met toestemming OvJ-EU demaskeren	**169**
	PIU- PIU Spontaan (art 10 PNR lid 2)	
1.6	Ontvangen verzoeken van PIU	
1.6.1	Aantal spontane verstrekkingen aan PIU op grond van vergelijking met databank of criteria	**0**
	PINL – PIU (art 14 PNR lid 1)	
1.8	Aantal spontane verzoeken van PINL aan PIU	
1.8.1	Aantal spontane verzoeken	**0**
	PIU - PINL Extra pushes (art 11 PNR)	
1.9	Aantal ontvangen PIU verzoeken om extra push van luchtvaartmaatschappijen aan PINL	
1.9.1	Aantal ontvangen verzoeken van PIU om extra NL push	**0**
1.10	PINL - PIU Extra pushes (art 15 PNR lid 1)	
1.10.1	Aantal naar PIU verstuurde Pi-NL-verzoeken extra push van luchtvaartmaatschappij	**0**
	BIEU - PINL – BIEU (art 10 PNR lid 4 jo art 13 PNR)	
1.11	BIEU verzoeken met dringende noodzaak rechtstreeks aan PINL	
1.11.1	Aantal BIEU-verzoeken aan Pi-NL	**4**
1.11.2	Aantal BIEU-verzoeken met toestemming OvJ demaskeren	**4**
1.11.3	Aantal door PINL verzonden afschriften van verzoek BI EU aan PIU	**0**
	Europol - PI-NL – Europol (art 10 PNR lid 4 jo art 13 PNR)	

1.12	Aantal verzoeken van Europol (via DLIO/Siena) aan PINL (art 12 PNR lid 1)	
1.12.1	Aantal ontvangen verzoeken van Europol	**100**
1.12.2	Aantal verzoeken met toestemming OvJ demaskeren	**24**
	3e land - PI-NL - 3e Land (art 13 PNR lid 1)	
1.13	Aantal verstrekkingen door PINL aan 3e land van PNR-data	
1.13.1	Aantal ontvangen verzoeken van 3e land	**19**
1.13.2	Aantal verzoeken met toestemming OvJ demaskeren	**7**
1.13.3	Verzoek om toestemming PIU verzonden door PINL aan PIU	**0**
	PIU - PINL - 3e Land (art 13 PNR lid 2)	
1.14	Aantal verstrekkingen door PINL aan 3e land van data van andere PIU zonder voorafgaande toestemming PIU	**0**
1.14.1	Notificatie verzonden door PINL aan PIU	**0**
2	**Verstrekkingen**	
2.1	Totalen algemeen	
2.1.1	Totaal aantal verstrekkingen	**24.180**
2.1.1	Aantal verstrekkingen op grond van vordering	**16.743**
2.1.3	Aantal verstrekkingen op grond van databank (SISII)	**6.600**
2.1.4	Aantal verstrekkingen op grond van criteria	**837**
2.1.5	Aantal verstrekkingen van gedemaskeerde persoonsgegevens	**6.397**
	BINL - PINL (art 9 PNR)	
2.2	Aantal verstrekkingen van PINL aan BINL	
2.2.1	Aantal verstrekkingen van PINL aan BINL	**15.357**
2.2.2	Aantal verstrekkingen van gedemaskeerde persoonsgegevens aan BINL	**5.799**
	BINL - PINL - PIU - PINL – BINL (art 14 PNR lid 2 en 3)	
2.3	Aantal verzoeken door PINL bij PIU t.b.v. BINL	
2.3.1	Aantal verstrekkingen van PIU via PINL aan BINL	**402**
2.3.2	Aantal verstrekkingen PIU van gedemaskeerde persoonsgegevens t.b.v. BINL	**0**

	BINL-PIU – BINL (art 16 PNR lid 1 en 2)	
2.4	Aantal door BINL rechtstreeks verstuurde verzoeken aan PIU in het kader van dringende noodzaak	
2.4.1	Van BINL ontvangen kopie van PIU-verstrekkingen	**0**
	PIU - PIU (art 10 PNR lid 2)	
2.5	Aantal verstrekkingen (via DLIO/Siena) aan PIU	
2.5.1	Aantal verstrekkingen (via DLIO/Siena) aan PIU	**1.624**
2.5.2	Aantal verstrekkingen van gedemaskeerde persoonsgegevens aan PIU	**443**
	PIU- PIU Spontaan (art 10 PNR lid 1 jo. art 6 lid 1 en 2)	
2.6	Aantal spontane verstrekkingen aan PIU op grond van vergelijking databank of criteria	
2.6.1	Spontane verstrekking van PINL aan PIU	**0**
2.7	Aantal door PINL ontvangen spontane verstrekkingen van PIU t.b.v. BINL doorgegeven aan BINL (art 9a PNR jo. 8 PNR)	
2.7.1	Aantal ontvangen spontane verstrekkingen van PIU	**0**
2.7.2	Aantal door PINL aan BINL doorgegeven spontane verstrekkingen van PIU	**0**
2.8	Aantal spontane verzoeken van PINL aan PIU (art 14 PNR lid 1)	
2.8.1	Aantal ontvangen spontane verstrekkingen van PIU	**0**
2.9	Aantal PINL-verstrekkingen van extra push van luchtvaartmaatschappijen aan PIU (art 11 PNR)	
2.9.1	Aantal PINL-verstrekkingen aan PIU van extra NL push	**0**
2.10	Aantal van PIU ontvangen PIU-verstrekkingen extra push van luchtvaartmaatschappij (art 15 PNR lid 1)	
2.10.1	Aantal verstrekkingen van PIU van extra PIU push aan PINL	**0**
	BIEU - PINL – BIEU (art 10 PNR lid 4 jo 13 PNR)	
2.11	PINL rechtstreekse verstrekkingen aan BIEU met dringende noodzaak	
2.11.1	Aantal verstrekkingen door PINL aan BI EU	**62**

2.11.2	Aantal verstrekkingen van gedemaskeerde persoonsgegevens aan BIEU	**45**
	Europol - PINL- Europol (art 12 PNR lid 1)	
2.12	Aantal verstrekkingen PINL (via DLIO/Siena) aan Europol	
2.12.1	Aantal PINL-verstrekkingen aan Europol	**474**
2.12.2	Aantal PINL-verstrekkingen van gedemaskeerde persoonsgegevens aan Europol	**94**
	3e land - PINL - 3e Land	
2.13	Aantal verstrekkingen door PINL aan 3e land van PNR-data (art 13 PNR lid 1)	
2.13.1	Aantal verstrekkingen door PINL aan 3e land	**63**
2.13.2	Aantal verstrekkingen van gedemaskeerde persoonsgegevens aan 3e landen	**16**
	PINL - 3e Land zonder voorafgaande toestemming PIU (art 13 PNR lid 2)	
2.14	Aantal verstrekkingen door PINL aan 3e land van data van andere PIU zonder voorafgaande toestemming PIU	
2.14.1	Aantal verstrekkingen PIU-verstrekkingen door PINL aan 3e land	**0**
2.14.2	Aantal verstrekkingen van gedemaskeerde persoonsgegevens aan 3e landen	**0**

5 Bijlagen

5.1 Lijst van passagiersgegevens[3]

1. PNR-bestandslocatie.
2. Datum van reservering en afgifte van het biljet.
3. Geplande reisdatum of -data.
4. Naam of namen.
5. Adres en contactgegevens, waaronder telefoonnummer en e-mailadres.
6. Alle betalingsinformatie, met inbegrip van het factuuradres.
7. Volledige reisroute voor dit specifieke PNR.
8. Informatie betreffende reizigers die gebruik maken van een loyaliteitsprogramma voor frequent reizen.
9. Reisbureau of reisagent.
10. Reisstatus van de passagier, met inbegrip van bevestigingen, check-in-status en «no-show» of «go-show»-informatie.
11. Opgesplitste of opgedeelde PNR-informatie.
12. Algemene opmerkingen, waar onder wordt begrepen alle beschikbare informatie over niet-begeleide minderjarigen jonger dan 18 jaar, zoals naam en geslacht van de minderjarige, leeftijd, talen die de minderjarige spreekt, naam en contactgegevens van de persoon die de minderjarige begeleidt naar het vertrek en de aard van de relatie van deze persoon met de minderjarige, naam en contactgegevens van de persoon die de minderjarige afhaalt bij aankomst en de aard van de relatie van deze persoon met de minderjarige, functionaris voor vertrek en aankomst.
13. Informatie uit de biljetuitgifte («ticketing field»-informatie), waaronder wordt begrepen het biljetnummer, de uitgiftedatum van het reisbiljet, biljettentickets voor enkele reizen en geautomatiseerde prijsnotering van reisbiljetten.
14. Zitplaatsinformatie, waaronder het zitplaatsnummer.
15. Informatie over gemeenschappelijke vluchtnummers.
16. Alle bagage-informatie.
17. Aantal en namen van de andere reizigers in het PNR.
18. Alle verzamelde API-gegevens (Advance Passenger Information), waaronder wordt begrepen soort, nummer, land van afgifte en geldigheidsdatum van een identiteitsdocument, nationaliteit, familienaam, voornaam, geslacht, geboortedatum, luchtvaartmaatschappij, vluchtnummer, datum van vertrek, datum van aankomst, luchthaven van vertrek, luchthaven van aankomst, tijdstip van vertrek, tijdstip van aankomst.
19. Alle vroegere wijzigingen in de onder de punten 1 tot en met 18 genoemde passagiersgegevens.

[3] Bijlage 1 bij PNR-wet

5.2 Lijst van strafbare feiten[4]

1. Deelneming aan een criminele organisatie.
2. Mensenhandel.
3. Seksuele uitbuiting van kinderen en kinderpornografie.
4. Illegale handel in verdovende middelen en psychotrope stoffen.
5. Illegale handel in wapens, munitie en explosieven.
6. Corruptie.
7. Fraude, met inbegrip van fraude ten nadele van de financiële belangen van de Unie.
8. Witwassen van opbrengsten van criminaliteit en valsemunterij, met inbegrip van namaak van de euro.
9. Computercriminaliteit/cybercriminaliteit.
10. Milieumisdrijven, met inbegrip van de illegale handel in bedreigde diersoorten en de illegale handel in bedreigde planten- en boomsoorten.
11. Hulp bij illegale binnenkomst en illegaal verblijf.
12. Moord, doodslag en zware mishandeling.
13. Illegale handel in menselijke organen en weefsels.
14. Ontvoering, wederrechtelijke vrijheidsberoving en gijzeling.
15. Georganiseerde en gewapende diefstal.
16. Illegale handel in cultuurgoederen, waaronder antiquiteiten en kunstvoorwerpen.
17. Namaak van producten en productpiraterij.
18. Vervalsing van administratieve documenten en handel in valse documenten.
19. Illegale handel in hormonale stoffen en andere groeibevorderaars.
20. Illegale handel in nucleaire of radioactieve stoffen.
21. Verkrachting.
22. Misdrijven die onder de rechtsmacht van het Internationaal Strafhof vallen.
23. Kaping van vliegtuigen/schepen.
24. Sabotage.
25. Handel in gestolen voertuigen.
26. Industriële spionage.

NB: naast bovenstaande ernstige misdrijven vallen ook de in artikel 83 en 83b van het Wetboek van Strafrecht benoemde terroristische misdrijven onder de doelbinding van de Pi-NL.

[4] Bijlage 2 bij de PNR-wet

5.3 Passagiersgegevens: API en PNR

Artikel 4 van de PNR-wet stelt dat een luchtvaartmaatschappij van elke vlucht aan de passagiersinformatie-eenheid de passagiersgegevens verstrekt waarover zij ten behoeve van haar bedrijfsvoering beschikt. Conform de bijlage bij de wet betreft dit de Passenger Name Records (PNR) en Advance Passenger Information (API) - voor zover de luchtvaartmaatschappij hier dus over beschikt.

PNR is de informatie die een luchtvaartmaatschappij nodig heeft om haar eigen bedrijfsproces goed te kunnen uitvoeren. Bijvoorbeeld de datum van reservering, contactgegevens, bagage-informatie en eventuele beschikbare check-in en boardinggegevens.

API is informatie die door overheidsinstanties wordt gebruikt voor hun (grens)toezichttaken; deze wordt dus specifiek door luchtvaartmaatschappijen met dit doel verzameld. API betreft de gegevens uit het reisdocument (zoals naam en nationaliteit), over de vlucht (zoals het vluchtnummer en tijdstip van vertrek) en over de reisroute.

Voor beiden soorten passagiersgegevens geldt dat er op grond van de PNR-richtlijn en PNR-wet geen *verzamelplicht* is voor luchtvaartmaatschappijen. Alleen de gegevens waarover zij reeds beschikken dienen te worden doorgestuurd aan de passagiersinformatie-eenheid.